



550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Telephone: 215.977.4100
Fax: 215.977.4101
www.lewisbrisbois.com

SIAN M. SCHAFLE
DIRECT DIAL: 215.977.4067
SIAN.SCHAFLE@LEWISBRISBOIS.COM

June 15, 2016

VIA ELECTRONIC MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Data Event

Dear Sir/Madam:

We represent Tom McLeod Software Corps ("TMSC"), 2550 Acton Road, Birmingham Alabama, 35243, and are writing to notify your office of an incident that affects the security of personal information relating to one (1) Maryland resident. By providing this notice, Tom McLeod Software Corps does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Nature of the Data Event

On June 8, 2016, TMSC discovered that it had been the victim of an email spoofing scam that resulted in a compromise of the security of employee 2015 IRS Tax Form W-2 information including employee names, addresses, Social Security numbers, and wage information. This incident occurred on June 7, 2016. Through this spoofing scam, a request had been made from what appeared to be a legitimate TMSC email address for 2015 employee W-2 information. Unfortunately, the W-2 information was provided prior to TMSC becoming aware of the fraudulent nature of the request. TMSC discovered the fraudulent nature of the request on June 8, 2016 and immediately began working diligently to investigate and to mitigate the potential impact of the incident.

Notice to Maryland Resident

On June 9, 2016, TMSC sent emails disclosing this incident to potentially impacted individuals for whom TMSC has valid email addresses. See *Exhibit A* as an exemplar of

this email communication. On June 10, 2016, TMSC supplemented the June 9, 2016 email to provide additional information on this incident, steps the impacted individuals may take to protect against potential identity theft and fraud, and access to one (1) year of free credit monitoring and identity theft restoration services through Experian. The supplemental email correspondence was sent to impacted TMSC employees in substantially the same form as the attached ***Exhibit B***. TMSC began notifying potentially affected individuals on June 14, 2016, which included one (1) Maryland resident. The notifications provide details of the incident, additional information on steps individuals can take to protect against identity theft and fraud, and contact information individuals may use should they have questions or concerns. The notice letters were provided in substantially the same form as the letter attached here as ***Exhibit C***.

Other Steps Taken and To Be Taken

Upon discovering this incident, TMSC moved quickly to identify those who may be affected, to put in place resources to assist them, and to provide them with notice of this incident. As noted above, TMSC is providing potentially affected individuals information on how to better protect against identity theft and fraud, including information on how to place a fraud alert or security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies and the IRS, and encouragement to contact the Federal Trade Commission, state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

TMSC has security measures in place to protect the security of information in its possession. As part of its ongoing commitment to the security of personal information, TMSC is working to implement additional protections and provide additional training on safeguarding the privacy and security of information in our systems. TMSC reported this incident to the IRS, the FBI, and local law enforcement. Additionally, while there is currently no indication a compromise to the security of its systems, TMSC analyzing its systems to confirm the security of its network.

Very truly yours,



Sian M. Schafle of
LEWIS BRISBOIS BISGAARD & SMITH LLP